

# Pinned algebraic distances determined by Cartesian products in $\mathbb{F}_p^2$

Giorgis Petridis

## Abstract

Let  $p$  be an odd prime and  $A \subseteq \mathbb{F}_p$  be a subset of the finite field with  $p$  elements. We show that  $A \times A \subseteq \mathbb{F}_p^2$  determines at least a constant multiple of  $\min\{p, |A|^{3/2}\}$  distinct pinned algebraic distances.

## 1 Introduction

Erdős proved in [5] that a finite planar set  $E \subset \mathbb{R}^2$  determines at least  $\Omega(|E|^{1/2})$  distinct distances and conjectured it determines at least  $|E|^{1-o(1)}$ . The conjecture was proved by Guth and Katz after decades of partial progress in their seminal paper [7]. The corresponding conjecture for distances “pinned” at some point of  $E$  remains open, with the best known bound being due to Katz and Tardos [14].

The question has been studied in the context of two-dimensional vector spaces over finite fields, where the algebraic distance between two points  $u = (u_1, u_2)$  and  $v = (v_1, v_2)$  is defined as

$$\|u - v\| = (u_1 - v_1)^2 + (u_2 - v_2)^2.$$

For notational brevity we denote the set of algebraic distances determined by  $E$  by

$$\Delta(E) = \{\|u - v\| : u, v \in E\}$$

and the set of algebraic distances determined by  $E$  pinned at some  $u \in E$  by

$$\Delta_u(E) = \{\|u - v\| : v \in E\}.$$

---

The author is supported by the NSF DMS Grant 1500984.

The algebraic structure of vector spaces  $\mathbb{F}_q^2$  is very different to  $\mathbb{R}^2$  and so peculiarities arise. For example, if  $-1$  is a square in the field, say  $i^2 = -1$ , then the *isotropic line*  $\{(t, it) : t \in \mathbb{F}_q\}$  determines only one distance: 0. Subfields also pose obstructions to improving upon an Erdős type lower bound  $|\Delta(E)| = \Omega(|E|^{1/2})$ , which can be obtained once  $E$  is not contained in an isotropic line : If  $E$  is the Cartesian product of a subfield, then  $\Delta(E)$  is precisely the subfield and so  $|\Delta(E)| = |E|^{1/2}$ .

Bourgain, Katz, and Tao worked over prime order fields  $\mathbb{F}_p$  where  $p$  is an odd prime congruent to 3 mod 4 (and so -1 is not a quadratic residue) in their ground breaking paper [2]. In this setting the above obstructions do not occur and Bourgain, Katz, and Tao proved there exists  $u \in E$  such that

$$|\Delta_u(E)| \geq |E|^{\frac{1}{2}+c}$$

for some  $c > 0$  that only depends on the cardinality  $|E|$ . Their proof was based on a point-line incidence theorem. An explicit  $c$  can be obtained by applying more recent point-line incidence results found in [1, 10, 12, 21]. Steven's and De Zeeuw's point-line incidence bound [21] in particular implies that, if  $E$  is not contained in an isotropic line and satisfies the hypothesis  $|E| = O(p^{11/15})$ , then there exists  $u \in E$  such that

$$|\Delta_u(E)| = \Omega\left(|E|^{\frac{1}{2}+\frac{1}{30}}\right).$$

For Cartesian products in  $\mathbb{F}_p^2$  (prime  $p$ ), Aksoy-Yazici, Murphy, Rudnev and Shkredov proved in [1] that  $E = A \times A$  determines  $\Omega(|E|^{\frac{1}{2}+\frac{1}{16}})$  algebraic distances if  $|E| = O(p^{16/15})$ . It is natural to also express their result as  $|\Delta(A \times A)| = \Omega(|A|^{9/8})$ . Inserting the point-plane incidence result of Steven's and De Zeeuw's [21] in the argument of Bourgain, Katz and Tao yields that there exists  $u \in A \times A$  such that

$$|\Delta_u(A \times A)| = \Omega(|A \times A|^{5/8}) = \Omega(|A|^{5/4}),$$

under the hypothesis  $|A \times A| = O(p^{4/3})$ . This is the best known bound in the literature.

The condition  $|E| = O(p^{4/3})$  that appears in the second result of Stevens and de Zeeuw from [21] is not restrictive. To see why one must investigate the complementary question of determining a lower bound on  $|E|$  so that  $\Delta(E)$  is as about large as it can ever be, which was first studied by Iosevich and Rudnev in [11]. Iosevich and Rudnev showed that  $|E| > 4q^{3/2}$  implies  $\Delta(E) = \mathbb{F}_q$ . Chapman, Erdoğan, Hart, Iosevich and Koh proved that  $|E| > q^{4/3}$  implies that  $\Delta(E)$  contains a positive proportion of the

elements of  $\mathbb{F}_q$  [3]. Hanson, Lund and Roche-Newton proved in [8] that under the same hypothesis  $|E| > q^{4/3}$  there exists  $u \in E$  such that the pinned distance set  $\Delta_u(E)$  contains a positive proportion of the elements of  $\mathbb{F}_q$ . Corresponding questions in  $\mathbb{F}_q^d$  for  $d \geq 3$  were studied in [9].

We prove a result on pinned algebraic distances for Cartesian products in  $\mathbb{F}_p^2$ , which goes beyond what can be achieved by current knowledge on point-line incidences and complements that of Hanson, Lund and Roche-Newton.

**Theorem 1.1.** *Let  $p$  be an odd prime and  $A \subseteq \mathbb{F}_p$ . There exist  $a, b \in A$  such that*

$$|\Delta_{(a,b)}(A \times A)| = \Omega(\min\{p, |A|^{3/2}\}).$$

Note that  $\Delta_{(a,b)}(A \times A) = \{(a - c)^2 + (b - d)^2 : c, d \in A\} = (A - a)^2 + (A - b)^2$  and that, in the notation used above, the theorem states there exists  $u \in E = A \times A$  such that  $\Delta_u(E) = \Omega(\min\{p, |E|^{3/4}\})$ .

Our proof is based on a simple averaging argument found, for example, in a paper of Chung, Szemerédi and Trotter [4] and a point-plane incidence theorem of Rudnev from [19]. So our method can be partly traced to the work of Guth and Katz (c.f. Section 2). It is possible to put the proof, which is reminiscent of an argument in [15], in the context of the main result of [1], but we opted for a more direct albeit longer presentation. It should also be noted that Theorem 1.1 would follow from the argument of Chung, Szemerédi and Trotter, only if there was in our disposal a point-line incidence bound comparable to what is known in  $\mathbb{R}^2$  [22].

**Acknowledgement.** I would like to thank Alex Iosevich and Misha Rudnev for generously sharing their insight.

**Notation.** We use Landau's notation so that both statements  $f = O(g)$  and  $g = \Omega(f)$  mean there exists an absolute constant  $C$  such that  $f \leq Cg$  and  $f = \Theta(g)$  stands for  $f = O(g)$  and  $f = \Omega(g)$ . The letter  $p$  denotes a prime,  $q$  a prime power,  $\mathbb{F}_q$  the finite field with  $q$  elements and  $\mathbb{F}_q^d$  the  $d$ -dimensional vector space over  $\mathbb{F}_q$ . An isotropic line is a line whose elements  $u$  satisfy  $\|u\| = 0$ . To make the proof easier to read, we do not use indicator functions and so write expressions like

$$\sum_{u,v,w \in E} 1_{\{\|u-v\|=\|v-w\|\}} = \sum_{u,v,w \in E} \{\|u-v\| = \|v-w\|\}.$$

## 2 Rudnev's point-plane incidences theorem

Given a point set  $P$  and a collection of planes  $\Pi$  in  $\mathbb{F}_p^3$ , a point-plane incidence is an ordered pair  $(u, \pi) \in P \times \Pi$  such that  $u \in \pi$ . Theorem 1.1 is a consequence of the following point-plane incidence bound of Rudnev [19]. We state the theorem in the simplest form adequate for our purpose.

**Theorem 2.1** (Rudnev). *Let  $p$  be an odd prime,  $P$  be a set of points in  $\mathbb{F}_p^3$  and  $\Pi$  be a set of planes in  $\mathbb{F}_p^3$ . Suppose that  $|P| = |\Pi| = O(p^2)$  and denote by  $k$  the maximum number of collinear points in  $P$ . The number of point-plane incidences is  $O(|P|^{3/2} + k|P|)$ .*

The proof of Rudnev's theorem has its roots in the solution to the Erdős distinct distance problem for planar sets by Guth and Katz [7] and the Klein–Plücker line geometry formalism [17, Chapter 2]. So it depends on classical techniques such as the polynomial method (see [6]), and properties of ruled surfaces (see [13]) and the Klein quadric (see [20]). Applying Theorem 2.1 in the setting of Theorem 1.1 is similar to how Theorem 2.1 was applied by Aksoy Yazici, Murphy, Rudnev and Shkredov in [1].

## 3 An averaging argument

The second ingredient to the proof of Theorem 1.1 is a simple observation that can be traced back at least to a paper of Chung, Szemerédi and Trotter [4] and which was first applied in the finite field context by Bourgain, Katz and Tao [2]. We state and prove it for sets in  $\mathbb{F}_q^2$ , though we only apply it in  $\mathbb{F}_p^2$ .

**Lemma 3.1.** *Let  $E \subseteq \mathbb{F}_q^2$  and  $N$  be the number of solutions to*

$$2u \cdot (v - w) + \|w\| - \|v\| = 0, \quad u, v, w \in E.$$

*There exists  $u \in E$  such that  $|\Delta_u(E)| \geq \frac{|E|^3}{N}$ .*

*Proof.* We begin by considering the quantity

$$\sum_{u \in E} \sum_{x \in \mathbb{F}_q} \left( \sum_{v \in E} |\{ \|u - v\| = x \}| \right)^2 = \sum_{u \in E} \sum_{x \in \mathbb{F}_q} \sum_{v, w \in E} |\{ \|u - v\| = x = \|u - w\| \}|$$

$$\begin{aligned}
 &= \sum_{u,v,w \in E} \sum_{x \in \mathbb{F}_q} |\{\|u - v\| = x = \|u - w\|\}| \\
 &= \sum_{u,v,w \in E} |\{\|u - v\| = \|u - w\|\}|.
 \end{aligned}$$

Standard properties of inner product imply

$$\|u - v\| = \|u - w\| \iff 2u \cdot (v - w) + \|w\| - \|v\| = 0$$

and so

$$\sum_{u \in E} \sum_{x \in \mathbb{F}_q} \left( \sum_{v \in E} |\{\|u - v\| = x\}| \right)^2 = N.$$

Therefore there exists  $u \in E$  such that

$$\sum_{x \in \mathbb{F}_q} \left( \sum_{v \in E} |\{\|u - v\| = x\}| \right)^2 \leq \frac{N}{|E|}.$$

$\Delta_u(E)$  is the support of the function  $x \rightarrow \sum_{v \in E} |\{\|u - v\| = x\}|$  and so by the Cauchy-Schwarz inequality:

$$|\Delta_u(E)| \geq \frac{\left( \sum_{x \in \mathbb{F}_q} \sum_{v \in E} |\{\|u - v\| = x\}| \right)^2}{\sum_{x \in \mathbb{F}_q} \left( \sum_{v \in E} |\{\|u - v\| = x\}| \right)^2} \geq \frac{|E|^2}{N/|E|} = \frac{|E|^3}{N}.$$

□

Note here that if  $E$  is an isotropic line, then  $N = |E|^3$ ; and if  $E = F \times F$  is the Cartesian product of a subfield  $F$ , then  $N = |F|^{5/2}$ .

Following Chung, Szemerédi and Trotter, Bourgain, Katz and Tao argued that for every pair of distinct  $v, w \in E$  that do not belong to an isotropic line, every  $u$  such that  $(u, v, w)$  contributes 1 to  $N$  belongs to the perpendicular bisector of  $v$  and  $w$ . So, when there are no isotropic lines, for each fixed  $w$  the number of  $(u, v)$  such that  $(u, v, w)$  contributes 1 to  $N$  equals the number of incidences between  $E$  and a family of  $|E| - 1$  lines. This means that improving the state-of-the art on point-line incidence bounds, gives improved bounds for  $N$  and consequently for the pinned distance set.

For Cartesian products we follow a different approach. We are able to avoid treating each  $w$  separately by reducing the question to one about point-plane incidences in  $\mathbb{F}_p^3$ .

## 4 Proof of Theorem 1.1

Recall that Theorem 1.1 states that for all  $A \subseteq \mathbb{F}_p$  there exist  $a, b \in A$  such that

$$|\Delta_{(a,b)}(A \times A)| = \Omega(\min\{p, |A|^{3/2}\}).$$

Lemma 3.1 reduces Theorem 1.1 to proving that  $N = O(|A|^{9/2} + |A|^6/p)$ , a bound in line with other applications of Rudnev's theorem [1, 16, 18]. As we will see below, the condition  $|P| = O(p^2)$  in Theorem 2.1 forces us to require  $|A| = O(p^{2/3})$ . For this technical reason, we prove the following claim.

**Claim.** Suppose that  $A \subseteq \mathbb{F}_p$  satisfies  $|A| = O(p^{2/3})$ . There exists  $u \in A \times A$  such that  $|\Delta_u(A \times A)| = \Omega(|A|^{3/2})$ .

The claim implies the theorem because, if  $A \subseteq \mathbb{F}_p$  has  $|A| = \Omega(p^{2/3})$ , then we pass to a subset  $A' \subseteq A$  with  $|A'| = \Theta(p^{2/3})$ . By the above, there exists  $u \in A'$  such that

$$|\Delta_u(A \times A)| \geq |\Delta_u(A' \times A')| = \Omega(|A'|^{3/2}) = \Omega(p).$$

Our first task in proving the claim is to express  $N$  using the coordinates of  $u, v, w$ , noting that the coordinates are elements of  $A$ .  $N$  is the number of solutions to

$$2u_1(v_1 - w_1) + 2u_2(v_2 - w_2) + (v_2^2 - w_2^2) = (v_1^2 - w_1^2) \quad u_i, v_i, w_i \in A.$$

We treat differently the case where  $v_1 = w_1$  or  $w_2 = w_2$ . Let us count the number of solutions where, say,  $v_1 = w_1$ . We must have  $v_2 = w_2$  or  $u_2 = -v_2 - w_2$ . In both cases there are at most  $|A|^3$  solutions (with  $v_1 = w_1$ ). Treating the case where  $v_2 = w_2$  identically we see there are at most  $4|A|^4$  solutions with  $v_1 = w_1$  or  $v_2 = w_2$ .

Assuming from now on that  $v_1 \neq w_1$  and  $v_2 \neq w_2$  we express the above equation as

$$(2u_1, v_2 - w_2, v_2^2 - w_2^2) \cdot (v_1 - w_1, 2u_2, 1) = v_1^2 - w_1^2, \quad v_i, w_i \in A, \quad v_i \neq w_i.$$

This reduces the question to a point-plane incidence bound for which we apply Theorem 2.1. The details are as follows.

*First step:* Define a set of distinct points

$$P = \{(2u_1, v_2 - w_2, v_2^2 - w_2^2) : u_1, v_2, w_2 \in A\}$$

and a family of distinct planes

$$\Pi = \{ \{x \in \mathbb{F}_q^2 : x \cdot (v_1 - w_1, 2u_2, 1) = v_1^2 - w_1^2\} : u_2, v_1, w_1 \in A \}.$$

Our choice of  $P$  and  $\Pi$  ensures that the number of point-plane incidences between  $P$  and  $\Pi$  is precisely the contribution to  $N$  coming from  $v_i \neq w_i$ .

*Second step:* The cardinalities of  $P$  and  $\Pi$  satisfy  $|P| = |\Pi| = |A|^3 - 2|A|^2 + |A| \leq |A|^3$ .

This is because, for distinct  $\alpha, \beta \in \mathbb{F}_p$ , the ordered pair  $(\alpha - \beta, \alpha^2 - \beta^2)$  determines uniquely the ordered pair  $(\alpha - \beta, \alpha + \beta)$ . Since the characteristic is odd, the ordered pair  $(\alpha - \beta, \alpha + \beta)$  determines uniquely the ordered pair  $(\alpha, \beta)$ . Moreover, since the characteristic is odd,  $2\alpha$  uniquely determines  $\alpha$ . The stated upper bound on  $|P|$  follows.

*Third step:* Our assumption that  $|A| = O(p^{2/3})$  implies that  $|P| = O(|A|^3) = O(p^2)$ .

*Fourth step:* The maximum number  $k$  of collinear points in  $P$  is at most  $2|A|$ . Recall that the elements of  $P$  are of the form  $(2u_1, v_2 - w_2, v_2^2 - w_2^2)$  with  $u_1, v_2, w_2 \in A$ ,  $v_2 \neq w_2$ . To show this we consider two different cases.

Lines not contained in any plane of the form  $\{X = \text{constant}\}$  intersect each plane  $\{X = 2u\}$  in at most one point. So they are incident to at most  $|A|$  points from  $P$ .

For lines contained in a plane of the form  $\{X = 2u\}$  we seek to bound the maximum number of collinear points of the form  $(v_2 - w_2, v_2^2 - w_2^2) \in \mathbb{F}_p^2$  with  $v_2, w_2 \in A$ . We distinguish between three types of lines:  $\{X = \text{constant}\}$ ,  $\{Y = \text{constant}\}$  and  $\{Y = mX + b\}$ . Lines of the form  $\{Y = \kappa\}$  are incident to at most  $2|A|$  elements of the form  $(v_2 - w_2, v_2^2 - w_2^2)$  with  $v_2, w_2 \in A$ , because for each  $v_2$  there are at most two  $w_2 \in \mathbb{F}_p$  such that  $v_2^2 - w_2^2 = \kappa$ . Similarly, lines of the form  $\{X = \kappa\}$  are incident to at most  $|A|$  elements of the form  $(v_2 - w_2, v_2^2 - w_2^2)$  with  $v_2, w_2 \in A$ . Finally, lines of the form  $\{Y = mX + b\}$  are incident to at most  $2|A|$  elements of the form  $(v_2 - w_2, v_2^2 - w_2^2)$  with  $v_2, w_2 \in A$ , because  $v_2$  and  $w_2$  must satisfy  $v_2^2 - w_2^2 = m(v_2 - w_2) + b$  and for each  $v_2$  there are at most two  $w_2 \in \mathbb{F}_p$  that satisfy the resulting quadratic equation.

*Fifth step:* Theorem 2.1 implies that  $N$ , which equals the number of point-plane incidences between  $P$  and  $\Pi$  plus  $O(|A|^4)$ , satisfies  $N = O(|A|^{9/2} + |A|^4) = O(|A|^{9/2})$ .

*Sixth step:* Lemma 3.1 implies that there exists  $u \in A \times A$  such that

$$|\Delta_u(A \times A)| \geq \frac{|A \times A|^3}{N} = \Omega\left(\frac{|A|^6}{|A|^{9/2}}\right) = \Omega(|A|^{3/2}) = \Omega(|A \times A|^{3/4}).$$

## References

- [1] E. Aksoy-Yazici, B. Murphy, M. Rudnev, and I.D. Shkredov. Growth estimates in positive characteristic via collisions. Accepted Int. Math. Res. Not. IMRN [arXiv:1512.06613](#), 2015. (pp. [2](#), [3](#), [4](#), and [6](#))
- [2] J. Bourgain, N.H. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14:27–57, 2004. (pp. [2](#) and [4](#))
- [3] J. Chapman, M.B. Erdoğan, D. Hart, A. Iosevich, and D. Koh. Pinned distance sets,  $k$ -simplices, Wolff’s exponent in finite fields and sum-product estimates. *Math. Z.*, 271(1-2):63–93, 2012. (p. [3](#))
- [4] F.R.K. Chung, E. Szemerédi, and W.T. Trotter. The number of different distances determined by a set of points in the Euclidean plane. *Discrete Comput. Geom.*, 7(1):1–11, 1992. (pp. [3](#) and [4](#))
- [5] P. Erdős. On sets of distances of  $n$  points. *Amer. Math. Monthly*, 53:248–250, 1946. (p. [1](#))
- [6] L. Guth. *Polynomial Methods in Combinatorics*. Amer. Math. Soc., Providence, R.I., 2016. (p. [4](#))
- [7] L. Guth and N.H. Katz. On the Erdős distinct distances problem in the plane. *Ann. of Math. (2)*, 181(1):155–190, 2015. (pp. [1](#) and [4](#))
- [8] B. Hanson, B. Lund, and O. Roche-Newton. On distinct perpendicular bisectors and pinned distances in finite fields. *Finite Fields Appl.*, 37:240–264, 2016. (p. [3](#))
- [9] D. Hart, A. Iosevich, D. Koh, and M. Rudnev. Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture. *Trans. Amer. Math. Soc.*, 363:3255–3275, 2011. (p. [3](#))
- [10] H.A. Helfgott and M. Rudnev. An explicit incidence theorem in  $\mathbb{F}_p$ . *Mathematika*, 57:135–145, 2011. (p. [2](#))
- [11] A. Iosevich and M. Rudnev. Erdős distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.*, 359:6127–6142, 2007. (p. [2](#))
- [12] T.G.F. Jones. An improved incidence bound for fields of prime order. *European J. Combin.* 52, 52:136–145, 2016. (p. [2](#))



- [13] N.H. Katz. The flecnode polynomial: A central object in incidence geometry. [arxiv:1404.3412](#), 2014. (p. 4)
- [14] N.H. Katz and G. Tardos. A new entropy inequality for the Erdős distance problem. In *Towards a theory of geometric graphs, Contemporary Mathematics 342*, pages 119–126. AMS, Providence, R.I., 2004. (p. 1)
- [15] B. Murphy and G. Petridis. A point-line incidence identity in finite fields, and applications. *Mosc. J. Comb. Number Theory*, 6(1):63–94, 2016. (p. 3)
- [16] G. Petridis. Products of differences in prime order finite fields. [arXiv:1602.02142](#), 2016. (p. 6)
- [17] H. Pottmann and J. Wallner. *Computational line geometry*. Springer-Verlag, Berlin, 2001. (p. 4)
- [18] O. Roche-Newton, M. Rudnev, and I.D. Shkredov. New sum-product type estimates over finite fields. *Adv. Math.*, 293:589–605, 2016. (p. 6)
- [19] M. Rudnev. On the number of incidences between planes and points in three dimensions. *Combinatorica*. To appear. (pp. 3 and 4)
- [20] M. Rudnev and J.M. Selig. On the use of the Klein quadric for geometric incidence problems in two dimensions. *SIAM J. Discrete Math.*, 2016. (p. 4)
- [21] S. Stevens and F. de Zeeuw. An improved point-line incidence bound over arbitrary fields. [arXiv:1609.06284](#), 2016. (p. 2)
- [22] E. Szemerédi and W.T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3–4):381–392, 1983. (p. 3)

Department of Mathematics, University of Georgia, Athens, GA, USA.

*Email address:* [giorgis@cantab.net](mailto:giorgis@cantab.net)